



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁴ : H04N 7/167, G07F 7/00 G07C 9/00		A1	(11) International Publication Number: WO 88/06826 (43) International Publication Date: 7 September 1988 (07.09.88)
(21) International Application Number: PCT/GB88/00151 (22) International Filing Date: 2 March 1988 (02.03.88) (31) Priority Application Number: 8704850 (32) Priority Date: 2 March 1987 (02.03.87) (33) Priority Country: GB		(74) Agent: R G C JENKINS & CO.; 26 Caxton Street, London SW1H 0RJ (GB). (81) Designated States: AT (European patent), BE (European patent), CH (European patent), DE (European patent), FR (European patent), GB (European patent), IT (European patent), JP, LU (European patent), NL (European patent), SE (European patent), US. Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>	
(71) Applicant (<i>for all designated States except US</i>): MARS INCORPORATED [US/US]; 6885 Elm Street, McLean, VA 22101-3883 (US). (72) Inventors; and (75) Inventors/Applicants (<i>for US only</i>): ARMOUR, James, Joseph [GB/GB]; Pine Cottage, Aldbourne Road, Baydon, Marlborough, Wiltshire (GB). GLASSPOOL, Andrew, Jim, Kelley [GB/GB]; 45 Alexandra Road, Addlestone, Surrey KT15 2PQ (GB).			
(54) Title: ACCESS SYSTEMS			
(57) Abstract			
<p>In an access system, preferably a conditional access TV broadcasting system, a key in a receiver stores a table of security codes and at pre-determined times starts to use a new one of the codes in order to generate an authorisation key for permitting access. The key also preferably stores a start time indicative of the first time that the key was used, and a lifespan indicative of the total duration for which it may be used. The lifespan is preferably shorter than the total period for which the stored security codes are valid.</p>			

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	FR	France	ML	Mall
AU	Australia	GA	Gabon	MR	Mauritania
BB	Barbados	GB	United Kingdom	MW	Malawi
BE	Belgium	HU	Hungary	NL	Netherlands
BG	Bulgaria	IT	Italy	NO	Norway
BJ	Benin	JP	Japan	RO	Romania
BR	Brazil	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	LI	Liechtenstein	SN	Senegal
CH	Switzerland	LK	Sri Lanka	SU	Soviet Union
CM	Cameroon	LU	Luxembourg	TD	Chad
DE	Germany, Federal Republic of	MC	Monaco	TG	Togo
DK	Denmark	MG	Madagascar	US	United States of America
FI	Finland				

- 1 -

ACCESS SYSTEMS

This invention relates to access systems in which access, e.g. to a service, a product or a location, is gained by means of an electronic key storing a security code. The invention is particularly but not exclusively concerned with conditional access television systems, e.g. for satellite broadcasting systems.

Various proposals for conditional access television systems are described in the Journal of the Institution of Electronic and Radio Engineers, Vol. 55, No. 11/12, pp.377 to 385, November/December 1985. Figure 4 on page 382 illustrates one such system, in which a transmitter transmits scrambled television picture and sound signals and encrypted control signals. In the receiver, the control signals are decrypted and used for descrambling the picture and sound signals. Decryption is carried out in a detachable sub-system (also referred to herein as a key). The sub-system stores a distribution key (also referred to herein as a security code) and a validation code which are combined to form an authorisation key used for decryption. The authorisation key corresponds to the one used in the transmitter for encrypting the control

signals.

Each user would have a different distribution key stored in his detachable sub-system. Periodically, the control computer alters the authorisation key, and, for each user who has paid his subscription, calculates a validation code from the new authorisation key and the user's distribution key. This validation code is broadcast, and the user's detachable sub-system receives and stores the validation code. Accordingly, anyone who fails to pay his subscription will not have his validation code renewed when the authorisation key is changed, and therefore the sub-system will no longer be able to decrypt the control signals so that the picture and sound signals cannot be unscrambled. Such an arrangement requires transmission of a large number of codes, and thus if there are many subscribers a large bandwidth is needed.

The above article also describes on page 384 an alternative pre-payment system, in which each detachable sub-system has a stored credit value and a stored expiry date. Instead of paying subscriptions, a user will pay for the services by buying a sub-system. As the sub-system is used, the stored credit value is decreased. When it reaches zero, or the expiry date is reached, the sub-system can no longer be used. The article states that this system does not require the use of validation codes.

Both the above techniques are subject to fraud, particularly by means of copying the sub-systems. It is proposed to mitigate this problem by making the sub-systems detachable and issuing new sub-systems when fraud is detected. However, this is an expensive solution, and it would not always be apparent when replacement of sub-systems is required.

According to one aspect of the present invention, a key for a controlled access system is operable to produce a security code to be used in determining whether access is provided to the system, wherein the key is operable to produce a different security code after a selected time.

The key, which for example could be detachable, and which could form a sub-system for a controlled access pre-payment television system, may be arranged so that the produced security code varies depending upon the current time (e.g. in dependence upon the date). The current time may be determined by signals generated by the television receiver, or by signals transmitted with a television signal.

By periodically changing the security code, the opportunity for anyone fraudulently to copy the key is reduced, and the value of the copy is reduced because the key will no longer be effective after the time at which the security code is due to change.

-4-

In such a system, it is envisaged that at predetermined times, preferably separated by at least a day, and more preferably several days, the security codes being produced by all keys or sub-systems for decrypting control signals used for descrambling television signals, and the code used by the transmitter to encrypt such control signals, would change in synchronism.

The invention is preferably embodied in a pre-payment system. If the system does not require the transmission of validation codes, the arrangement may be such that, at any given time, all the sub-systems used for receiving a particular broadcasting service generate the same security code.

The invention also extends to systems which use transmitted validation codes, e.g. subscription systems. Each sub-system may have a unique identity code, so that validation codes can be transmitted individually to the different sub-systems. In each sub-system, the validation code and the stored security code are used together to form an authorisation key to enable access (e.g. to enable de-scrambling of broadcast signals). Because the sub-system is only effective for a limited duration, it is no longer necessary for the system to transmit signals to the individual sub-systems in order to maintain them operational and, the end of the subscription, to disable them. Instead, the sub-system

-5-

automatically remains operational throughout the subscription period, and is automatically disabled at the end of the subscription by virtue of the fact that it will no longer store a security code appropriate for the current date. This substantially reduces the number of validation signals which need to be transmitted, and thus the bandwidth requirements are relaxed.

A second aspect of the invention is concerned with a modification of this arrangement. According to this second aspect, an access system comprises a plurality of sub-systems, each storing a security code and each arranged to receive a validation code, each sub-system being operable to permit access on condition that an authorisation key derived from the validation code and the security code is deemed appropriate, wherein the sub-systems are divided into groups according to expiry date, and wherein sub-systems within a group having a common expiry date also have a common security code. In this case also, the number of signals needed to be transmitted can be greatly reduced as compared with the prior art. In the preferred embodiments, only a single validation code is transmitted for each user in order to render his sub-system operational. Further validation signals may be directed to the sub-system, e.g. to maintain it operational and/or to disable it at the expiry date, but the same signals would be used by other sub-systems in

-6-

the same group, and therefore the total number of different signals needed to be transmitted is greatly reduced.

Of course in the above arrangements, as in the prior art, any signal which is transmitted is desirably repeated at intervals over a period to ensure that it has been received properly by all the sub-systems to which it is directed. However, unlike prior art systems, it is not necessary for this operation to be performed at regular intervals in order to maintain individual sub-systems operational throughout the subscription period and individually to disable the sub-systems at the end of the subscription period.

Arrangements embodying the invention will now be described with by way of example with reference to the accompanying drawing, in which:

Figure 1 is a schematic block diagram of an access system in accordance with the invention.

In the access system 2, which in this embodiment is a TV broadcasting system, picture signals delivered along a path 4 are scrambled by a picture signal scrambler 6 and then delivered to a transmitter 8. The transmitted signals are received by a receiver 10 which then delivers the scrambled picture signals to a descrambler 12. The descrambled picture signals are then presented to a display 14.

-7-

The scrambler 6 scrambles the signals according to a code generated by a scrambling controller 16. The code is also delivered to an encrypter 18, which encrypts the codes in accordance with an authorisation key received from a control computer 20. The encrypted codes form control signals which are delivered to transmitter 8 and transmitted along with the transmitted picture signal.

A receiver 10 separates the encrypted control signals from the picture signals and delivers them to a key or sub-system 22. Within the sub-system the control signals are delivered to a decrypter 24, in which they are decrypted in accordance with an access signal in the form of an authorisation key received from a sub-system controller 26. Normally, the authorisation key generated by the sub-system controller 26 should correspond to that generated by the control computer 20, and hence the control signals can be decrypted by the decrypter 24, whereby they can be used by the descrambler 12 in order to descramble the picture signals. Obviously sound signals can be treated in the same way.

The control computer 20 receives a signal indicative of the current time and date from a clock 28. This signal is used to determine which address in a memory 30 is accessed in order to obtain the authorisation key sent to the encrypter 18. The memory 30 stores a substantial number of authorisation keys which are used in

-8-

succession. By way of example, a new authorisation key may be used once a month.

In the sub-system 22, a signal indicative of the current time is delivered to the controller 26 on line 31. This signal may be generated by a clock in the receiving installation, or may be derived from signals transmitted by the transmitter 8. The controller 26 uses the time signal to determine which location in an authorisation key store 32 is read to derive the authorisation key sent to the decrypter 24.

The memory 32 stores a limited number of authorisation keys corresponding to those generated by the computer 20 over a limited period. Accordingly, once this period has expired, the sub-system 22 is no longer operable to enable correct descrambling of the picture signals.

In a simple embodiment, the period over which the sub-system 22 is useful is governed solely by what authorisation keys are stored in memory 32. Preferably, however, the sub-system 22 stores further information which places additional restrictions on the useful life of the sub-system 22. This further information may also be contained in the memory 32, and may include any or all of the following:

- (1) An expiry date. The controller 26 can compare this with the current date and not permit accessing of an

-9-

authorisation key if the current date is later than the expiry date.

(2) A start date. The controller 26 would compare this with the current time, and prevent the reading out of authorisation keys if the current time is prior to the start date. The start date could be programmed into the sub-system by the supplier.

(3) A lifespan. The controller would check whether the sub-system has been used for a period longer than the lifespan, and if so would prevent reading out of the authorisation keys. To achieve this, the sub-system would record the time at which it was first used. This could be accomplished by using the programmed start date referred to in paragraph (2). Alternatively, the sub-system could be arranged automatically to record the time at which it is first used.

The advantages of such an arrangement are that it allows essentially the same sub-system to be used in different circumstances, e.g. to cover different periods of use. For example, the sub-system could contain authorisation keys suitable for a period of 15 months, together with a lifespan of 12 months. This would allow the sub-system to have a shelf life of 3 months within which it could be purchased and still provide 12 months of use. If the lifespan, start date, and/or expiry date are

-10-

programmable by the supplier he will be able to determine the periods for which the sub-system may be used. These parameters are preferably stored in the form of units corresponding to the period between changes in authorisation key by the control computer 20. For example the start date could be recorded as the value "4" if the first authorisation key to be used by the sub-system is that corresponding to the fourth time period for which the authorisation keys stored in memory 32 are valid.

It will be understood that a system according to the present invention has the advantage over the prior art pre-payment system described above, in that there is a risk that the prior art system could be "fooled" into thinking that the expiry date has not yet been reached by interfering with the signals supplied to the sub-system which are intended to indicate the current time. In the present system, this would result in the sub-system producing the wrong security code, so that fraudulent reception of the service could not be achieved by this means.

In addition to or instead of the authorisation keys being selected according to the current date, means are preferably provided to determine whether an authorisation key is valid so that the controller 26 could perform a search operation in which authorisation keys are successively selected until the correct one is

- 11 -

chosen. To this end, an encrypted version of the correct authorisation key could be transmitted, and the sub-system could compare the decrypted version with its generated authorisation key to determine if the latter is valid.

Also or alternatively, a different authorisation key could be selected in response to a command broadcast by the transmitter 8. Accordingly, if it is found that the security system has been breached and that fraudulent access is being gained to the system, the security codes can be changed without requiring the users' sub-systems to be returned to a distributor and without requiring new sub-systems to be issued.

It is desirable that successive security codes produced by a key or sub-system have no readily discernible relationship between them. The key may be arranged to look up the security code (or a value which is used to calculate the security code) in a stored table, the look up location being determined at least in part by the current time. Alternatively, the key could be arranged to generate the security code using an algorithm dependent at least in part upon the current time. It is however preferred that the security codes be produced using a look-up table, because using an algorithm to generate the security codes results in a risk that the algorithm will be discovered to enable the fraudulent generation of security codes.

-12-

In an alternative embodiment the authorisation key sent by the controller 26 to the decrypter 24 is determined in dependence on both a security code accessed from the memory 32 and a validation code stored in a further memory 34. This validation code has been derived from the control signals transmitted by the transmitter 8. The validation codes are transmitted to individual sub-systems. For this purpose they are transmitted along with addresses which correspond to unique identification numbers stored in the sub-systems. Accordingly, as is per se known in the art, the memory 34 will receive only the validation code which is appropriate for the particular sub-system for which it is installed. The validation code is generated by the control computer 20 prior to transmission, and for this purpose a database 36 storing customer details and sub-system identification numbers is used.

In a further alternative, instead of each individual sub-system having a unique security code, the sub-systems can be arranged in groups sharing a common security code. Preferably, the sub-systems are divided into groups according to expiry date, and sub-systems within the same group use a common security code at any given time. The security code is combined with a validation code stored in the memory 34 to generate the authorisation key. An individual validation code is

-13-

transmitted to a user when he first starts to use the sub-system to render his sub-system operational. Thereafter group messages are sent at regular intervals to all sub-systems having the same expiry date to maintain them operational, e.g. by transmitting the validation code appropriate for the next period. The messages are the same for all sub-systems within the group, and different from those sent to other groups. As the expiry date for a group approaches, no further enabling messages are sent to that group.

Similarly, the sub-systems could be divided or subdivided geographically, such that sub-systems for use in the same geographical area have the same security code.

In a still further modification, instead of all sub-systems storing corresponding tables of security codes, each stores only a single security code which is common to the group.

The sub-systems described above could be easily modified to store a conventional security code in addition to the security codes referred to above so that the same sub-system can be used in a conventional manner for reception of one channel and in one of the ways described above for reception of another channel.

If validation codes are transmitted, they can contain information used to control the manner in which access is provided. For example, they could control which

-14-

channels the sub-system is enabled for, and specific periods within which to enable them. Alternatively, they could contain keys used to decipher transmitted control signals determining the manner of access.

The decrypter 24 shown in Figure 1 could alternatively lie outside the sub-system 22.

In pre-payment conditional access systems, it has been proposed that the sub-system should provide a signal in dependence upon whether there is any remaining credit stored in the sub-system, and an enabling signal which is used only if the credit-indicating signal is present for enabling access, e.g. by descrambling broadcast television systems. According to another aspect of the present invention there is provided a conditional access system in which a key or sub-system is operable to generate enabling signals for enabling access only on condition that the sub-system stores a credit value. Thus, once the credit reaches zero, no enabling signals are generated and fraudulent access cannot be achieved by generating a false credit-indicating signal. For this purpose, the sub-system 22 of Figure 1 stores a credit value (e.g. in memory 32) which is automatically decremented as the sub-system is used, and the controller 26 accesses a security code only if the value is greater than zero.

-15-

The sub-system 22 is shown in Figure 1 as having several functional blocks, including controller 26, decrypter 24, memory 32 and, optionally, memory 34. Although each of these blocks can be formed by respective circuits, it is preferred that the sub-system be formed by a microprocessor having a single memory and arranged to perform all the necessary functions. Thus, the access signal could be a multi-bit word transmitted to a decrypter, or could simply be a stored data value used by the microprocessor in performing a decryption function.

Although the present invention has been described primarily in connection with a sub-system which generates an authorisation key for decrypting control signals transmitted with a television signal, other techniques are possible. The control signals may be generated locally, rather than being broadcast by the television signal transmitter, or the signals from the sub-system could be used directly for descrambling television signals rather than decrypting control signals which are then used for descrambling. The authorisation keys produced by the sub-system may be used for other purposes than descrambling. In addition to satellite broadcasting, the invention is useful also in terrestrial broadcasting and cable systems.

Of course the invention is also applicable to systems other than broadcasting systems. For example,

-16-

the system could be used for controlling access to buildings, computers e.t.c. It is particularly useful where access is dependent upon the current time, e.g. for shift workers, because the security code produced by the key may be selected according to the current time.

It is preferred that the key or sub-system described above be detachable, and preferably portable. Devices which are particularly suitable for use as the key are the tokens described in published patent applications GB-A-2153128 and GB-A-2196450 and GB patent application 8626233. However, some aspects of the invention are useful also with non-detachable sub-systems.

- 17 -

CLAIMS:

1. A key for a controlled access system, the key being operable to produce a security code to be used in determining whether access is provided to the system, wherein the key is operable to produce a different security code after a selected time.
2. A key as claimed in claim 1, including means responsive to a signal indicative of the current time for determining the security code to be generated.
3. A key as claimed in claim 1 or claim 2, including a memory storing a plurality of selectable security codes.
4. A key as claimed in any preceding claim, the key being operable to determine whether the produced security code is valid, and if not to produce said different security code.
5. A key as claimed in any preceding claim, the key storing data determining a duration within which it is operable to produce a security code of a type which permits access.

6. A key as claimed in any preceding claim, the key being automatically operable to store an indication of the time at which it first generated a security code permitting access.
7. An access system having a key as claimed in any preceding claim.
8. An access system as claimed in claim 7, comprising a distribution station and a plurality of receiving stations, each having a respective key as claimed in any one of claims 1 to 6.
9. An access system as claimed in claim 8, wherein each key is operable to generate an authorisation key signal determining whether access is provided and dependent on both a security code and a validation code received from the distribution station.
10. An access system as claimed in claim 9, wherein the keys are divided into groups within each of which the keys have a respective common expiry date and a respective common security code.

-19-

11. An access system comprising a distribution station and a plurality of receiving stations each having a respective key for selectively permitting access to the system in dependence on whether or not an authorisation key signal generated by the key is appropriate, wherein the authorisation key signal is determined in dependence on both a validation code received from the distribution station and a security code, and wherein the keys are divided into groups within each of which the keys have a respective common expiry date and a respective common security code.
12. An access system as claimed in any one of claims 8 to 11, wherein the distribution station is a TV broadcasting station, and wherein each receiving station is operable to unscramble picture signals on condition that the respective key generates an access signal permitting access to the system.
13. An access system substantially as herein described with reference to the accompanying drawing.

1/1

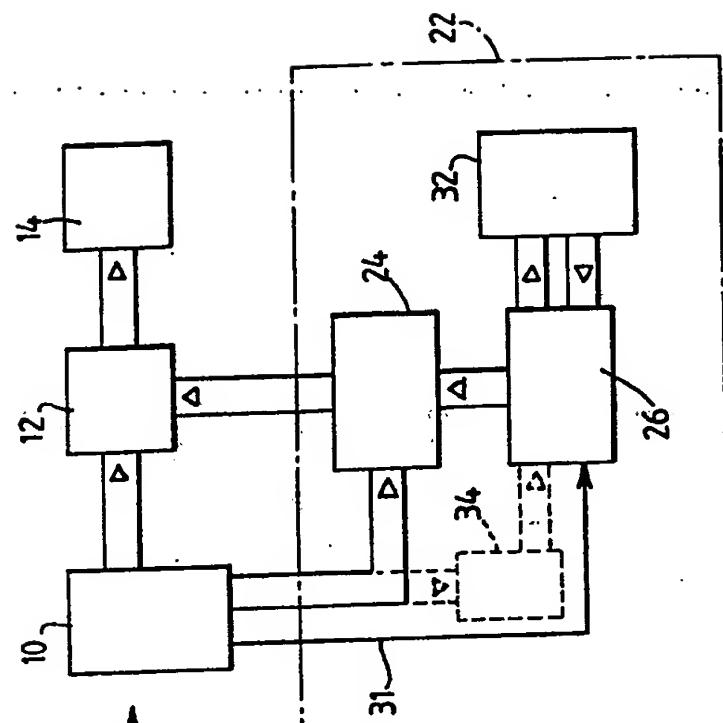
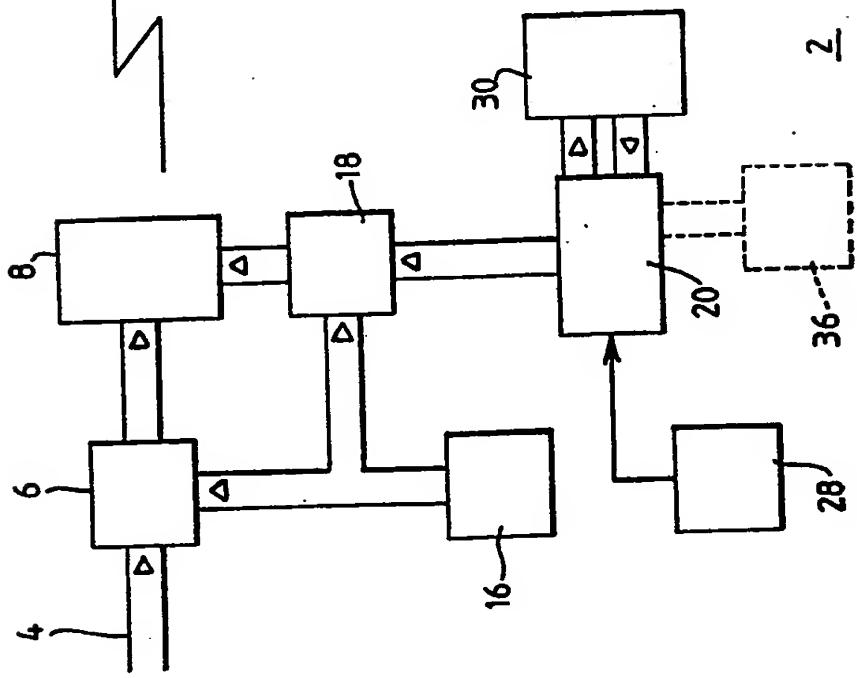


Fig.1.



INTERNATIONAL SEARCH REPORT

International Application No PCT/GB 88/00151

I. CLASSIFICATION OF SUBJECT MATTER (If several classification symbols apply, indicate all) *

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC⁴: H 04 N 7/167; G 07 F 7/00; G 07 C 9/00

II. FIELDS SEARCHED

Minimum Documentation Searched ?

Classification System	Classification Symbols
IPC ⁴	H 04 N; G 07 F; G 07 C

Documentation Searched other than Minimum Documentation
to the Extent that such Documents are Included in the Fields Searched *

III. DOCUMENTS CONSIDERED TO BE RELEVANT*

Category *	Citation of Document, ¹¹ with indication, where appropriate, of the relevant passages ¹²	Relevant to Claim No. ¹³
X	WO, A, 85/03785 (GORDIAN SYSTEMS) 29 August 1985, see abstract; page 2, line 11 - page 3, line 2; page 4, lines 4-11; page 18, line 1 - page 20, line 10; claims 1,2; figures	1,2,7
Y		11,12
A	--	6,10
X	Journal of the Institution of Electronics and Radio Engineers, vol. 55, no. 11/12, November/December 1985 S.M. Edwardson: "A conditional access system for direct broadcasting by satellite", pages 377-385, see chapter 5-7;11.2; figures	1,7-9,13
Y		11,12
A	--	10
	(cited in the application)	
	--	

* Special categories of cited documents: 10

"A" document defining the general state of the art which is not
considered to be of particular relevance

"B" earlier document but published on or after the international
filing date

"C" document which may throw doubt on priority claim(s) or
which is cited to establish the publication date of another
citation or other special reason (as specified)

"D" document referring to an oral disclosure, use, exhibition or
other means

"E" document published prior to the international filing date but
later than the priority date claimed

"F" later document published after the international filing date
or priority date and not in conflict with the application but
cited to understand the principle or theory underlying the
invention

"G" document of particular relevance; the claimed invention
cannot be considered novel or cannot be considered to
involve an inventive step

"H" document of particular relevance; the claimed invention
cannot be considered to involve an inventive step when the
document is combined with one or more other such documents,
such combination being obvious to a person skilled
in the art

"I" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search
1st June 1988

Date of Mailing of this International Search Report
07 JUL 1988

International Searching Authority

Signature of Authorized Officer

EUROPEAN PATENT OFFICE

P.C.G. VAN DER PUTTEN

III. DOCUMENTS CONSIDERED TO BE RELEVANT (CONTINUED FROM THE SECOND SHEET)		
Category	Citation of Document, with indication, where appropriate, of the relevant passages	Relevant to Claim No
A	EP, A, 0178809 (WIEDEMER) 23 April 1986, see abstract; page 5, line 3 - page 6, line 7; page 21, line 4 - page 22, line 9; claims; figures	1,3,5-13
A	EP, A, 0153837 (MATSUSHITA) 4 September 1985, see abstract; page 6, line 5 - page 7, line 9; page 10, line 9 - page 11, line 15; page 14, line 19 - page 16, line 12; page 31, line 9 - page 32, line 19; figures	1-13
A	EP, A, 0127381 (M/A-COM LINKABIT) 5 December 1984, see page 2, line 19 - page 7, line 8; page 8, line 6 - page 9, line 21; page 44, line 18 - page 46, line 25; figures	1,7,8,10-13
A	EP, A, 0137960 (NEC) 24 April 1985, see abstract; page 17, lines 10-26; figures	1,2,11
A	EP, A, 0021938 (BABONNEAU) 7 January 1981, see page 7, line 11 - page 10, line 10; figures	1,7,11

ANNEX TO THE INTERNATIONAL SEARCH REPORT
ON INTERNATIONAL PATENT APPLICATION NO.

GB 8800151
SA 20983

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report.
The members are as contained in the European Patent Office EDP file on 23/06/88.
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO-A- 8503785	29-08-85	AU-A- 4062685 EP-A- 0172239 JP-T- 61501291 US-A- 4599489 US-A- 4609777		10-09-85 26-02-86 26-06-86 08-07-86 02-09-86
EP-A- 0178809	23-04-86	JP-A- 61095688 US-A- 4696034		14-05-86 22-09-87
EP-A- 0153837	04-09-85	JP-A- 60171880 AU-A- 3864285 AU-B- 559311 JP-A- 60171885 JP-A- 60171886 JP-A- 60171883		05-09-85 22-08-85 05-03-87 05-09-85 05-09-85 05-09-85
EP-A- 0127381	05-12-84	AU-A- 2870784 JP-A- 60057783 US-A- 4613901 AU-B- 559463 DE-A- 3470368		29-11-84 03-04-85 23-09-86 12-03-87 11-05-88
EP-A- 0137960	24-04-85	JP-A- 60043790 DE-A- 3466846 JP-A- 60080378		08-03-85 19-11-87 08-05-85
EP-A- 0021938	07-01-81	WO-A- 8002901 FR-A, B 2459595 US-A- 4354201 CA-A- 1167562		24-12-80 09-01-81 12-10-82 15-05-84